UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/415,293	10/08/1999	EARL T. CARTER	062891.0324	4623

7590 09/30/2003

SCOTT T MORRIS
BAKER & BOTTS LLP
2001 ROSS AVENUE
DALLAS, TX 752012980

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2132	7

DATE MAILED: 09/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/415,293	CARTER, EARL T.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Response to Arguments

1. This communication is in response to applicant' amendment received on July 14, 2003. Claims 1, 7 and 13 are amended and claims 14-20 are newly added. Also some parts of the specification are amended.

2. Applicants' arguments have been fully considered but they are not persuasive.

3. Applicant's arguments are all in relation to the new limitations added to claims 1, 7 and 13 and the newly added claims 14-20. Therefore, the applicant's arguments are responded in the context of rejecting these claims as follows.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 7, 13-14 and 20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

6. There is no explanation for the following expressions in the specification of the claimed invention:

Claim 1, lines 7-8, claim 7, lines 9-10, claim 13, lines 4-5, claim 14, lines 8-9 and claim 20, line 6:

"**at a binary state machine prior to being buffered at a first network device.**"

Claim 1, lines 10-11, claim 7, lines 20-22, claim 13, lines 23-24, claim 14, lines 11-12, claim 20, lines 7-8:

"**storing a copy of the input stream at a network interface disposed between the first network device and the second network device.**"

Claim 1, lines 16-17, claim 7, lines 18-19, claim 13, lines 22-23, claim 14, line 17, claim 20, lines 12-13:

"**discarding the first character before selecting a next character of the input stream".**

Claim 1, lines 18-19, claim 7, lines 23-24, claim 13, lines 25-26, claim 14, lines18-19, claim 20, lines 14-15:

"**transmitting the copy of the input stream to the first network device if an attack on the computer network is not detected**.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 1-5, 7-18 and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Hile et al. (5,319,776) (hereinafter Hile).

With respect to claims 1, 7, 14 and 20, Hile discloses:

"Maintaining a state table". See, for example, column 2, lines 36-42.

"The state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an indication of an attack on a computer network". See, for example, column 4, line 59-column 5, line 21 where the machine state at start is zero and every next state and every incoming

character are corresponding to the recited current state and current character, respectively, which are applied (inputted) to the state table to determine the next state of the machine. At the end, if checking of all characters of a string results in a predetermined machine state a virus match (intrusion detection) has occurred (indication of an attack).

"Maintaining the current state". See, for example, Figure 3, where after each comparison step the resulting new state is maintained to be used as a current step for the next comparison step.

"Receiving an input stream at a binary state machine prior to being buffered at a first network device, the input stream comprising a plurality of characters transmitted by a second network device." See, for example, column 4, lines 47-58 and further Hile discloses that the input stream coming from a source medium to a destination medium (see, for example, Fig. 1) is checked character by character in the state machine 32 before being stored in the buffer 38 of the destination 24b (see column 4, lines 7- 26). There is also another buffer (buffer 30 in Fig. 1) in Hile's system that is located prior to the state machine 32. The buffer 30 only holds one or more blocks of data that is in transit and not store them permanently (see column 3, line 61-column 4, line 6). The size of this buffer is not that large (just holding some blocks of data) to be considered as a storage of the whole incoming data from the source medium. It is apparent that these few blocks of data stay in the buffer 30 for a short duration of time which is equal to the period of time that it takes state machine to inspect them. Thus this arrangement of

Hile's system satisfies the limitation of receiving an input stream at a binary state machine prior to being buffered at a first network device.

The holding of one or more blocks of data in the buffer 30 of Hile's system until they are string searched for virus signature corresponds to the recited limitation of "storing a copy of the input stream at network interface disposed between the first network device and the second network device."

"Selecting a first character of the input stream as the current character; comparing a current character and the current state to the state table to generate a new state". See, for example, column 4, line 66-column 5, line 20.

The process of searching through a string of characters as disclosed by Hile for determining whether a virus signature exist in the input stream (see column 4, line 59-column 5, line 21) which is very similar to the claimed invention by applicant corresponds to the recited limitation of "discarding the first character before selecting a next character of the input stream."

Hile also discloses that the input stream is transmitted to the destination medium if no virus signature detected in the stream (column 2, lines 12-35). Thus, the blocks of data that are being hold temporarily in the buffer 30 are transmitted to buffer 38 of the destination medium.

Referring to claims 2 and 15, Hile discloses:

"Initializing the current state to an initial state". See, for example, column 4, lines 64-66.

Referring to claims 3, 11 and 16, Hile discloses:

"Setting the current state equal to the new state; selecting a next character as the current character, the next character appearing subsequent to the first character in the input stream; and repeating the comparing step". See, for example, column 4, line 59-column 5, line 21.

Referring to claims 4, 12 and 17, Hile discloses:

"Recognizing the new state as indicative of an attack upon the computer network". See, for example, column 5, lines 17-21.

Referring to claims 5 and 18, Hile discloses:

"Sounding an alarm". See, for example, column 4, lines 16-22.

Referring to claim 8, Hile discloses:

"A computer readable medium, wherein the state table is stored upon the computer readable medium". See, for example, column 2, lines 4-7 and lines 36-42, column 3, lines 24-26 and column 4, lines 13-16.

Referring to claim 9, Hile discloses:

"The state machine comprises software code stored upon the computer readable medium, the software code further operable to be executed by a computer processor".

See, for example, column 2, lines 36-42, column 4, lines 48-50 and column 5, lines 22-30.

Referring to claim 10, Hile discloses:

"The state machine is further operable to initialize the current state to an initial state". See, for example, column 4, lines 64-66.

Referring to claim 13, this claim is rejected as applied to the like elements of claims 1, 7, 14 and 20 above and further the following.

Hile discloses:

"A computer readable medium". See, for example, column 2, lines 4-7 and column 3, lines 24-26.

"A network interface for receiving an input stream comprising a plurality of characters". See, for example, column 1, lines 19-32.

"A processor communicatively coupled to the computer readable medium and the network interface". See, for example, column 2, lines 25-27 and lines 36-40, column 3, lines 17-24 and column 7, lines 39-44.

"A state table stored upon the computer readable medium, the state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an attack on a computer network". See, for example, column 4, lines 13-16 and column 4, line 59-column 5, line 21 where the machine state at start is zero and every next state and every incoming character are

corresponding to the recited current state and current character, respectively, which are applied (inputted) to the state table to determine the next state of the machine. At the end, if checking of all characters of a string results in a predetermined machine state a virus match (intrusion detection) has occurred (indication of an attack).

"A state machine comprising instructions stored upon the computer readable medium and executable by the processor". See, for example, column 4, line 56-column 5, line 20.

"The state machine communicatively coupled to the state table". See, for example, column 2, line 36-42.

"The state machine operable to: maintain the current state". See, for example, Figure 3, where after each comparison step the resulting new state is maintained to be used as a current step for the next comparison step.

"Select a first character of the input stream as the current character and compare the current character and the current state to the state table to generate a new state". See, for example, column 4, line 66-column 5, line 20.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to

a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 6 and 19 are rejected under 35 USC 103(a) as being unpatentable over Hile et al. (5,319,776) (hereinafter Hile) in view of Ainsbury et al (6,078,924) (hereinafter Ainsbury).

11. Referring to claims 6 and 19, Hile does not expressly discloses:

"Generating the state table from a REGEX command". Ainsbury teaches that the REGEX (Regular Expression) are used to form tables. The Regular Expressions are commonly used in the art for parsing tables. See, for example, column 49, lines 57-67 and column 50, line 57-column 51, line 67.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the use of REGEX to generate state tables as taught in Ainsbury with the system of Hile, because it would provide state tables to be parsed by REGEX command to identify a pattern of character string.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar
Examiner
Art Unit 2132

A. N.

AN
September 23, 2003

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100